ICT for peace FOUNDATION

CYBER POLICY PROCESS BRIEF

ENEKEN TIKK-RINGAS

DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATION IN THE CONTEXT OF INTERNATIONAL SECURITY: **WORK OF THE UN FIRST COMMITTEE 1998-2012**

2012

Eneken Tikk-Ringas (2012) Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012, ICT4Peace Publishing, Geneva.

Copies available from www.ict4peace.org.

INTRODUCTION

With the UN General Assembly convening the third time[1] a Group of Governmental Experts (GGE) in 2012 to address threats to international information security in the Disarmament and International Security Committee (also known as the First Committee), this brief summarizes the work done by the First Committee in the field of international information security, highlights key national positions[2] and discussion and looks at the challenges facing the upcoming GGE discussions.

The Disarmament and International Security Committee (also the First Committee) is one of the six so-called 'main' committees enabling the General Assembly to 'parallel process' items on its agenda during each session. Holding permanent status since 1956, the First Committee deals with international peace and security and is suited to evaluate aspects of information security that could pose a threat to international peace and security and, consequently, could, upon national initiative, go before the Security Council for an actual enforcement action.

The past activities of the First Committee include international concerns of nuclear nonproliferation, chemical and biological weapons and weapons of mass destruction. Further, the disarmament of outer space and prevention of a space arms race has been addressed by the First Committee, as well as issues involving regional security and terrorism.

INCEPTION

The first tabling by Russia of developments in the field of information and communications in the context of international security with the First Committee in 1998 was hardly fortuitous. After years of pursuing strict control over the acquisition of advanced technology by the Eastern Bloc[3] the US had focused on the commercial potential of the Internet[4] while at the same time increasingly integrating information and communication technologies (ICTs) into its military doctrine[5]. Following an unsuccessful attempt to negotiate a bilateral presidential statement on international information security with the US[6], Russia selected the UN as one of the key forums to promote international information security.[7]

A special letter[8] was sent by the Minister of Foreign Affairs of the Russian Federation to the UN Secretary-General in September 1998, accompanied by a draft resolution on "Developments in the field of information and telecommunications in the context of international security" (hereinafter the Resolution). The initial draft of the Resolution proposed an 'inventory of information technologies' in order to 'prevent military

1 The first GGE met 2004-2005 and the second GGE 2009-2010. The meetings of the third GGE are scheduled to August 6-10, 2012 (New York), January 14-18, 2013 (Geneva) and June 3-7, 2013 (New York).

2 For a detailed list of national positions, see also UNIDIR (2012) A Review of Previously Submitted Contributions on Information Security.

3 US national policy on the transfer of scientific, technical and engineering information (1985). Available http://www.fas.org/irp/offdocs/nsdd/nsdd-189.htm.

4 Presidential Directive on Electronic Commerce. July 1, 1997.

5 Joint Doctrine for Information Operations (1998). Available http://www.c4i.org/jp3_13.pdf.

6 The Joint Statement on Common Security Challenges at the Threshold of the Twenty-First Century from September 2, 1998 was significantly briefer on information security than the Russian Delegation had hoped. For an overview of the intent, see Andrey V. Krutskikh, Advancement of Russian Initiative to Ensure International Information Security (Chronicles of the Decade), in "The International Information Security: The Diplomacy of Peace. Compilation of Publications and Documents" (2009).

7 Russia also pursued its interests in other international and regional organizations, including the Council of Europe Committee of Experts on Terrorism (CODEXTER) and the Shanghai Cooperation Organization.

8 A/C.1/53/3 - Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General. The text of the letter is annexed to this brief.

applications thereof that may be compared to the use of weapons of mass destruction'.[9]

A month later Russia introduced an edited version of the Resolution[10] to the First Committee and after further minor revisions[11] the General Assembly adopted the Resolution[12] by consensus.

INHERENT ISSUES

From the beginning a deep and constructive discussion of international information security in the UN First Committee has been challenged by principally different approaches to "information security" by the US and other liberal democracies on one side and the Shanghai Cooperation Organization (SCO) countries on the other. Disagreement extends to key definitions; exact scoping of the topic; threat perception as well as the mandate and role of the UN in general and the First Committee in particular in resolving international information security issues.

Russia's definition of international information security promotes stability and elimination of threats to both information and communication infrastructure and the information itself.[13] Liberal democracies have taken a principled position on Freedom of Expression grounds against the notion that concepts of security should include the information itself, and have focused exclusively on the security of infrastructure and networks.[14]

Having avoided defining terms like "information security", "information network and infrastructure security"[15] and "cybersecurity"[16], the US has emphasized information security as an aspect of global communications, economic cooperation and trade, intellectual property rights, law enforcement, anti-terrorist cooperation and international peace and security[17] and promoted ensuring the reliability, availability and integrity of national and global information networks. On a separate note the US[18] has pointed out that the general topic of information security is much larger than projected for the First Committee.

The Resolution addresses criminal, terrorist and military uses of ICTs. On the one hand this has led to several countries[19] focusing their replies to aspects of general telecommunications and criminal uses of ICTs, of which others[20] have simply noted that these issues have already been addressed by other forums.

Conceptual differences extend to perceived threats to information and telecommunications in the context of international security. In the

9 Ibid.

10 A/C.1/53/L.17.

11 A/C.1/53/L.17/Rev.1.

12 A/RES/53/70.

13 Information area is defined as the sphere of activity involving the creation, transformation or use of information, including individual and social consciousness, the information and communication infrastructure and information itself (A/54/213). Similar definitions have later been adopted in the Agreement (see footnote 58) and in the Convention on International Information Security conceptualized by th Russian ministry of Foreign Affairs in 2011 (Available http://www.mid.ru).

14 US A/59/116/Add.1: Implicit in these proposals would be the extension to Governments of the right to approve or ban information transmitted into national territory from outside its borders should it be deemed disruptive politically, socially or culturally; Poland A/55/140/Add.1., UK A/59/116.

15 A/59/116/Add.1.

16 US A/66/152. The same term has also been adopted in UK's reply from 2004 (A/59/116) with reference to the principles of the World Summit on the Information Society.

17 US A/54/213, A/59/116/Add.1. Similar points have been made by Australia (A/54/213).

18 US A/54/213.

19 E.g. Guatemala A/57/166, El Salvador A/58/373, Argentina, Costa Rica, Georgia A/59/116, A/59/116, Qatar and United Arab Emirates A/61/161, Brunei Darussalam and Burkina Faso A/62/98, Brunei Darussalam A/62/98/Add.1., Niger A/63/139, Thailand and Ukraine A/64/129, Spain A/64/129/Add.1., Turkmenistan A/66/152/Add.1.

20 Australia and the US A/54/213, Sweden A/56/164, UK A/59/116.

face of Russia and a few others conceptualizing information itself as a weapon[21], some countries analogizing the potential danger posed by information weapons and information warfare to those of weapons of mass destruction[22] and western block has hardly touched upon the issue of information warfare and weapons, principally rejecting the need for disarmament and non-proliferation and emphasizing the criminal misuse of IT is a challenge to the interests of all States.[23]

With differing views as to the object and nature of the threat, it is not surprising that countries also disagree about the role of the First Committee in addressing international information security. Russia and others[24] have projected the UN and the First Committee as an appropriate forum to address a wide spectrum of threats to include military, terrorist and criminal uses of ICT, whereas the United States, Australia and the EU countries[25] have been willing to accept a more limited role of the First Committee in information security.[26]

Russia has emphasized 'obvious need' for international legal regulation of the worldwide development of civilian and military information technology. Others have opined that a legal instrument that would restrict the development or use of certain civil and/or military technologies is unnecessary[27] and that the law of armed conflict is applicable to military applications of information technologies.[28] Further countries have agreed with the need to develop international principles to address information security.[29] Still others have emphasized the applicability of other international norms in the field of information security.[30]

In the absence of a common understanding about the scope and focus of information security both in the context of the First Committee discussions and on a more global scale, the US has proposed that formulation of overarching principles pertaining to information security in all its aspects would be premature, that 'a substantive amount of systematic thinking' is needed before going further.[31] Brazil has recommended that the issue of criminal and terrorist activities be separated from that of cyberwarfare and the potential need for disarmament and non-proliferation.[32]

THE PROCESS FROM 1999 TO 2003

With the US, Australia and the EU countries particularly unenthusiastic about engaging in a debate about disarmament in the context of ICT, the process, between 1999 and 2004,

21 Russia A/54/213: /.../use of information to the detriment of a State's defence, administrative, political, social, economic or other vital systems, and the mass manipulation of a State's population with a view to destabilizing society and the State. References to uses of information as a weapon have also been made by Philippines A/56/164, Kazakhstan A/64/129, Mali (A/64/129/Add.1., Cuba A/65/154.

22 Russia A/54/213, Philippines A/56/164. Panama has noted that an attack in which new information and telecommunications technologies are employed may cause more damage than, for instance, a conventional bombardment (A/57/166/Add.1.).

23 US A/54/213, UK A/59/116, US A/59/116/Add.1.

24 Belarus and Cuba A/54/213, Syria A/57/166/Add.1., China A/59/116, Qatar A/63/139.

25 Sweden has submitted its replies on behalf the States members of the European Union that are also members of the United Nations.

26 Australia, UK A/54/213, Sweden A/56/164. The US has pointed out that the general topic of information security includes aspects that relate to international peace and security (the work of the First Committee) (A/54/213).

27 The US A/59/116/Add.1., UK A/59/116

28 Ibid. Also Mali A/64/129/Add.1.

29 Oman A/54/213, Mexico A/56/164, Syria A/57/166/add.1., Bolivia A/61/161, Burkina Faso A/62/98, Kazakhstan A/64/129.

30 Cuba A/58/373, China A/61/161, A/62/98, Mali A/64/129/Add.1.

31 US A/54/213 and A/59/116/Add.1.

32 Brazil A/60/95/Add.1.

mainly involved written input[33] from national governments not engaging in a deeper discussion on the topic in the First Committee.

In 2001, after two years of sponsoring the Resolution, Russia proposed the establishment of a special group of governmental experts (GGE) to consider existing and potential threats in the sphere of information security, possible cooperative measures, and to conduct a study of international information security issues. This proposal was followed up with a list of issues to be addressed by the group.[34] Russia expected to 'give the international community a unique opportunity to examine the entire range of issues involved' as 'no generally accepted appropriate international standards or instruments exist dealing with questions of information security from the standpoint of measures to reduce existing and potential global threats to information security'.[35]

In response, the US reiterated that the key threats to cyber security are criminal attacks by organized crime, individual hackers and non-State actors, including terrorists. 'The benefits of cyberspace can best be protected by focusing both on the effective criminalization by States of the misuse of information technology and on the systematic national implementation of measures designed to prevent damage to critical information infrastructures no matter the source of the threat'.[36] With respect to military applications of information technology, the US considered an international convention to be 'completely unnecessary' as 'the law of armed conflict and its principles of necessity, proportionality and limitation of collateral damage already govern the use of such technologies'.[37]

Remaining generally skeptical about the role of the First Committee in international information security discussions, the US, supported by Australia and the EU countries[38], suggested that the GGE's efforts should be informed by recent multilateral efforts to enhance regional cyber security, such as those of the Asia-Pacific Economic Cooperation Telecommunications Forum, the Organization of American States, the World Summit on the Information Society and the G8.[39]

Several countries supported assigning the UN should with the tasks related to a wide array of information security aspects[40]. Still others pointed out the potential of bilateral arrangements.[41]

2004 GGE

In June 2004 the first GGE convened with experts appointed by the Secretary-General on the basis of equitable geographical distribution.[42] The group comprised 15 nations including Belarus, Brazil, China, France, Germany, India, Jordan, South Korea, Malaysia, Mali, Mexico, Russia, South Africa, United Kingdom and the United States.[43]

As A.V. Krutskikh, the Russian diplomat

33 The Resolution invited states to inform the Secretary-General of their views and assessments on (a) general appreciation of the issues of information security; (b) definition of basic notions related to information security, (c) the context of relevant International concepts aimed at strengthening the security of global information and telecommunication systems and, as of 2006, (d) possible measures that could be taken by the international community to strengthen information security at the global level.

34 Russia A/58/373.

35 Russia A/58/373.

36 US A/59/116/Add.1.

37 US A/59/116/Add.1. In this context, also note the work of the Third Committee on combating the criminal misuse of information technologies and the Second Committee on creation of a global culture of cyber security.

38 Australia, UK A/54/213, Sweden A/56/164.

39 US A/59/116/Add.1.

40 Belarus and Brunei A/54/213, China and Lebanon A/59/116, Venezuela A/59/116/Add.1, Qatar A/65/154.

41 E.g. Australia A/54/213, Poland A/55/140/Add.1.

42 A/RES/58/32.

43 See Table 1 for the composition of the UN GGE during 2004-2012.

chairing the first (and later the second) GGE has observed, the work of experts was characterized by significant differences on key aspects of international information security[44] with Russia, China, Brazil and Belarus promoting the right of States to ensure their own information security without limitations and the adoption of a new international regime and the US and 'European countries' rejecting any references to disarmament in the report.[45]

The considerable differences of views contributed to the failure to adopt a consensus report. In a procedural report, Krutskikh referred to 'very limited time in which to consider a whole range of comprehensive issues that are confronting the international community with fundamentally new and sensitive problems'.[46] He concluded that 'even with the use of translation, the members of the GGE spoke different languages with respect to essential issues related to international information security' and that 'various States have different laws regulating issues related to ensuring information security and cyber security'.[47] Krutskikh further noted 'differing interpretations of current international law in the area of international information security'.[48]

Despite the difficulties faced by the first GGE, Russia proposed to continue 'consideration of international information security in all its aspects' and offered to resume the work of the GGE, encouraging the participation of States in the group who did not have the opportunity to participate from 2004-2005.[49]

After the first GGE process, the dynamics of the First Committee discussions on international information security changed considerably. Russia opened the resolution for co-sponsorship, while the United States started voting against it in subsequent years. Between 2005 and 2008 the US was the sole country to vote against the Resolution that attracted 30 co-sponsors during the same time[50].

2009 GGE

In the face of Russia favoring enlarging the group[51], the UN GA decided that the GGE, to begin work in 2009, be set up under the same principles as the first one.[52] The members of the 2009 GGE included Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, South Korea, Qatar, Russia, South Africa, United Kingdom and the United States.

The second GGE convened under rather different circumstances than its predecessor five years earlier. Estonia had suffered a cyber incident of national security relevance in 2007[53], Georgia had witnessed cyber attacks accompanying kinetic warfare[54] and Lithuania, after suffering politically motivated cyber incidents in 2008, had reported that it regarded cyber security as an important element of its national security[55]. All these incidents had happened under the circumstances of political tension between the victim nations and Russia and in every case, government level statements had been made about Russia's involvement in the incidents.[56]

With the Obama administration having adopted a cooperative approach to international

44 Krutskikh, 6, page 126.

45 Ibid.

46 A/C.1/60/PV.13.

47 Ibid.

48 Ibid.

49 A/C.1/60/PV.13

50 See table 2 for a list of countries having sponsored the Resolution from 2006 to 2011.

51 Ibid.

52 A/RES/60/45

53 See more in Eneken Tikk, Kadri Kaska, Liis Vihul. International Cyber Incidents: Legal Considerations, CCD COE Publishing, Tallinn (2010). Available at www.ccdcoe.org.

54 Ibid.

55 Lithuania A/64/129.

56 Georgia A/65/152.

security[57] the US had engaged in bilateral discussions on cyber security with Russia and China, who, along with Kazakhstan, the Kyrgyz Republic, Tajikistan and Uzbekistan had signed an information security agreement under the patronage of the Shanghai Cooperation Organization.[58] NATO was beginning to consider cyber threats of military relevance.[59]

Despite continuing differences regarding binding agreements[60] and the need to address non-state actors,[61] the second GGE resulted in a general recognition of the existence of international security relevant information security threats.

The main takeaways from the second GGE were a consensus to continue discussing norms pertaining to State use of ICTs, to reduce collective risk and protect national and international infrastructure. Further, the countries recommended confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including further exchange of national views on the use of ICTs in conflict.[62]

Recommendations also met the request of several nations to elaborate common terms and definitions relevant to the Resolution.[63] Further, information exchange on national legislation and national ICT security strategies, policies and best practices were recommended as well as identification of measures to support capacity-building in less developed countries.[64]

KEY DEVELOPMENTS AND POSITIONS SO FAR

Having regarded the First Committee as a rather remote forum for discussing information security[65] a decade ago, and initially doubting its role as a self-standing discussion venue[66], nations have over time acknowledged the niche of the First Committee in dealing with information security threats of international security relevance. By its mandate, position and membership, the First Committee is a unique forum for discussing the 'high end' of information security threats.

With over 50 nations having contributed[67] to the First Committee discussions on international information security over the past 15 years, the key strategic players in the process have been Russia and the United States, each having gathered a coalition of like-minded partners.

Additionally, a series of bilateral talks and programs related to security in the context of uses of ICTs have been initiated between Russia, China and the United States as well as between several other UN countries.[68]

In September 2011, China, Russia, Tajikistan

57 The U.S. International Strategy for Cyberspace (2011), available: www.whitehouse.gov.

58 Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, signed in Yekaterinburg on 15 June 2009.

59 NATO's Cyber Defence Policy and Concept were adopted in 2007 and 2008.

60 US and the coalition of like-minded continuously rejected the need for a treaty whereas Russia insisted on the need for a binding agreement and common terms and definitions. China rejected the applicability of the *jus ad bellum* and *jus in bello* in the sphere of information threats.

61 US A/54/213: The actions and programmes of Governments are by no means the only appropriate focus, for information security also involves important concerns of individuals, associations, enterprises and other organizations active in the private sector, also US A/59/116/Add.1.

62 A/65/201.

63 Qatar A/54/213, Russia, Philippines, Mexico A/56/164, Ukraine A/58/373, Bolivia A/61/161, Brazil A/64/129.

64 A/65/201.

65 US A/54/213, Sweden A/56/164.

66 Australia A/54/213. UK A/59/116.

67 Tables 1-3 specify the involvement of different nations (GGE membership, sponsorship of the Resolution or governmental replies).

68 Further bilateral and multilateral processes had been initiated, involving Brazil, South Africa, India, Australia, Canada and others.

and Uzbekistan submitted to the UN GA a proposal for an International Code of Conduct for Information Security.[69] A US House Resolution earlier this year has called on the Obama administration to oppose the Code of Conduct[70].

One of the few points all countries seem to have accepted is the general need for international cooperation and collaboration for the purposes of global information security. With the definition of the latter still open, the scope and nature of cooperation is still to be defined.

Governments also seem, in principle, have acknowledged state responsibility for acts and omissions in the field of information security[71] and noted that insufficient protection of vital resources and systems may pose a threat to national and international security.[72]

Many governments have accepted the applicability of existing law to international information security issues, although sometimes questioning the consistency of its application.[73] More recently, proposals have been tabled on developing politically binding norms of acceptable state behavior in cyberspace.[74] Russia, having pointed out 'the obvious need for international legal regulation'[75] in the past, has recently taken a more flexible approach and acknowledged the possibility of a soft law approach[76].

69 A/66/359.

70 H. CON. RES. 114, March 26, 2012.

71 US A/54/213, Russia (A/55/140), Sweden A/56/164.

72 Poland A/55/140/Add.1., Sweden A/56/164, Ukraine A/58/373.

73 US A/54/213; A/66/152, Ukraine A/58/373, UK A/65/154, Australia A/66/152, Netherlands A/66/152.

74 Germany, Netherlands, Australia A/66/152.

75 Russia A/55/140, Cuba A/54/213; A/58/373.

76 A.V. Krutskikh at a conference (Шестой международный научный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении информационной безопасности и противодействии терроризму») in Garmisch-Partenkirchen, Germany (April 23-26, 2012).

Some governments have emphasized the right of every country to protect its information and telecommunication systems (the terms and definitions differ by governments)[77], often with additional emphasis on the consistency of such measures with the sovereign rights of other nations.[78] The extent of national sovereignty remains an open question with China having stated that each government has the right to manage its own cyberspace in accordance with its domestic legislation[79].

LOOKING FORWARD – THE 2012-13 GGE

With experts from Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, United Kingdom and the United States the third GGE is now preparing to make a contribution that would produce useful and actionable input for national governments.

The lessons learned from the first and second GGE underline the need for better focusing the discussions on international peace and security. This would give the discussions in the First Committee greater weight and legitimacy among the international community and allow them to add a substantive layer to the work done in other forums. With additional discussion on confidence building measures (CBMs) in the OSCE and the ASEAN Regional Forum and bilaterally between selected nations, a more constructive dialogue on CBMs and their effect on international information security is feasible.[80]

77 Russia A/55/140 'information resources and vital structures'; Philippines A/56/164 'information resources'; Sweden A/56/164 'information and information-based systems';

78 Cuba A/54/213. Russia A/55/140, Venezuela A/59/116/Add.1

79 China A/62/98.

80 Also on the issue of CBMs, see Arvind Gupta (2012) CBMs in Cyber Space: What should be India's Approach? Available http://www.idsa.in/idsacomments/CBMsinCyberspace_ArvindGupta_270612.

While the 'language issue' could, theoretically, be overcome by developing a glossary for the group or simply defining the terms used in the next report, it is also likely that countries' positions will over time align in proportion with systematic thinking about uses of ICTs in the context of international peace and security.

To produce added value, the GGE would need to take into account relevant parallel processes in other organizations and their implications on international peace and security. It might be worthwhile to clearly separate the issues of criminal and terrorist uses of ICTs from those directly relevant to international peace and security and adjust the request for national views and assessments accordingly.

In the absence of verifiable data about relevant threats and incidents of international security relevance, expert discussions in the First Committee will run the risk of oversimplification, or, in contrast, excess complexity and emotion. In this context, national input on specific national and international peace and security concerns related to the use of ICTs could be requested and considered in the future work of the First Committee.

Also, there are a few outstanding issues from the previous phases of discussions, likely to continue to be addressed. It is expected that the legal issues (such as the applicability of the law governing the use of force, the law of armed conflict, implementation and interpreting of the legal concepts of sovereignty and state responsibility) will form a considerable part of the third round of GGE discussions. Also relevant for national and international peace and security might be a discussion of activities that might not invoke the applicability of *jus ad bellum*/*jus in bello*, but might breach customary international law on state responsibility or neutrality.

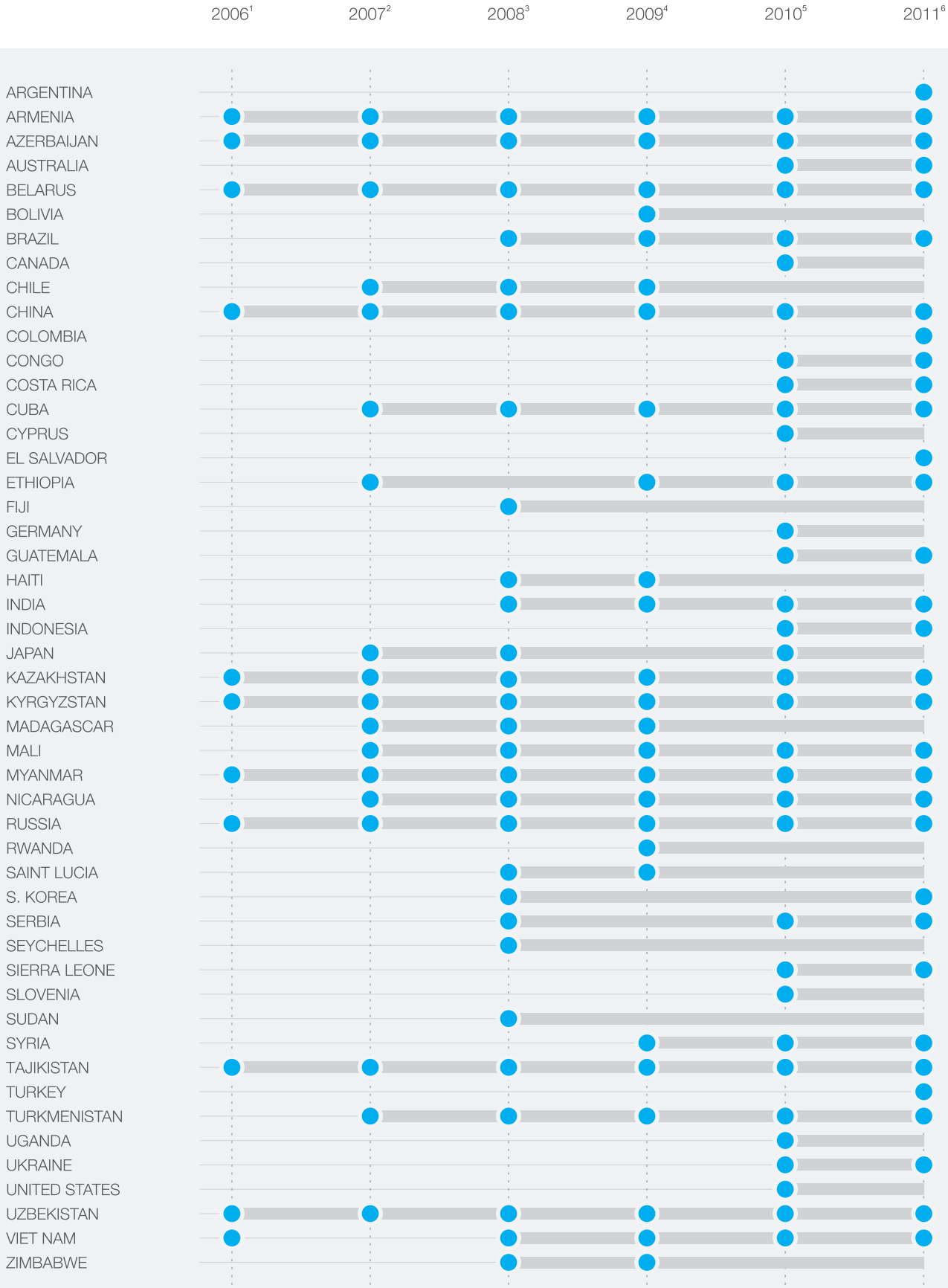
Another open issue, maybe less evident from the perspective of the mandate of the First Committee is the division of information security tasks between national governments and the international community. Several countries have pointed out the protection of information and information-based systems as a responsibility for governments[81], while others have emphasized the need for international cooperation and collective measures.

Further, the disagreement between the US-lead wing and the SCO countries on the Internet governance model is likely to shape discussions. In sum, although overall responsibility with respect to state-on-state behavior is with governments, taking action depends on close working with elements of the private sector, e.g. ISPs, companies involved in providing critical national infrastructure.

Somewhat surprisingly, issues often addressed in non-diplomatic forums, such as the threshold to justify the involvement of the Security Council or, potentially, self-defense by the victimized nations, the qualification of (and appropriate responses to) cyber attacks against national critical (information) infrastructure and avoiding the escalation of conflict under limited attribution, have so far not been tabled in the First Committee. In face of frequent governmental concerns about cyber incidents of national and international security relevance and along with the refinement of the First Committee mandate the GGE and governments may want to be prepared to discuss these issues in a not so distant future.

81 E.g. US A/54/213, Sweden A/56/164.

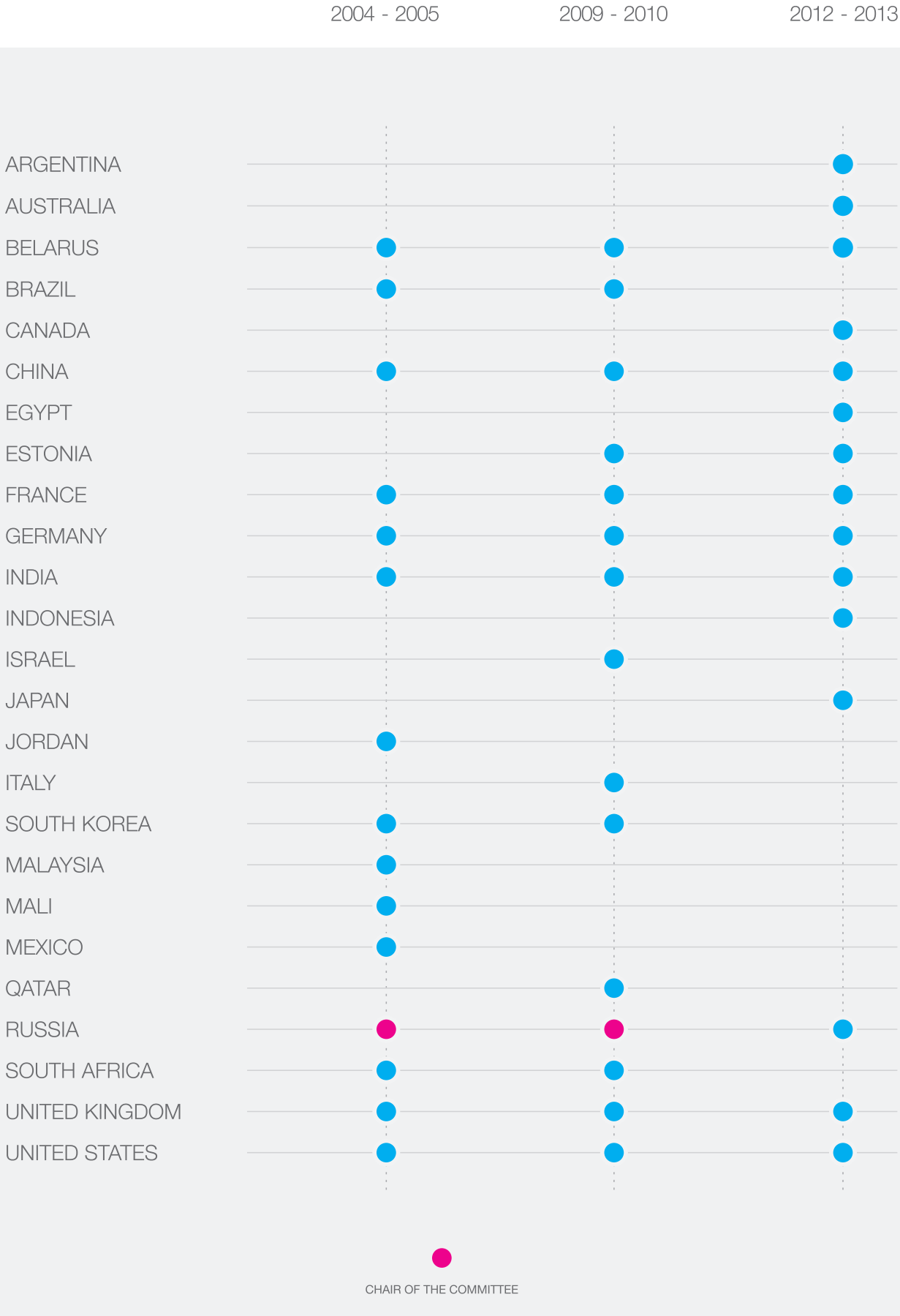
SPONSORS* OF THE RESOLUTION



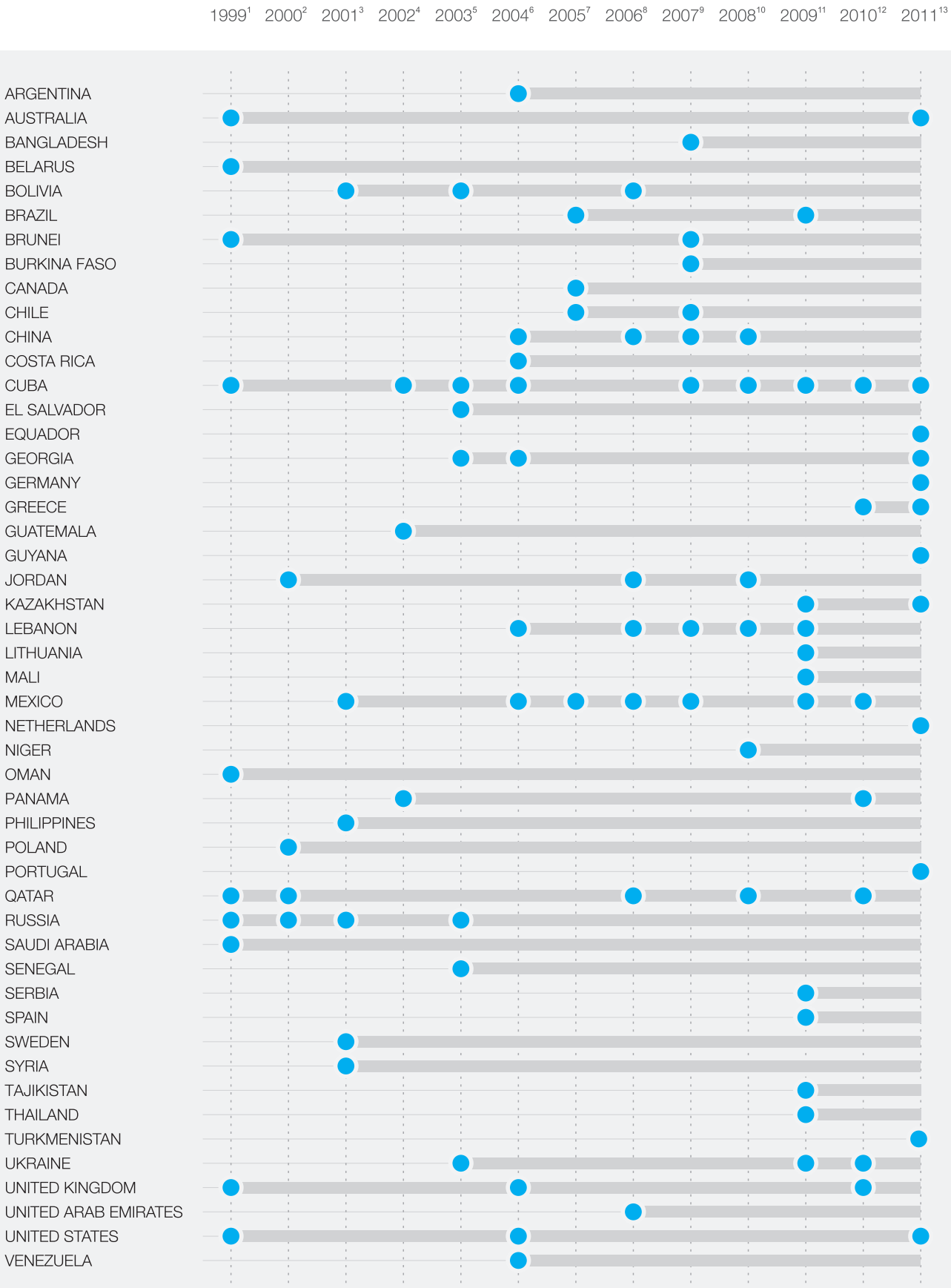
* the Resolution, authored and initiated by the Russian Federation in 1998, was opened for co-sponsorship in 2006

[1]A/61/389 [2]A/62/386 [3]A/63/385 [4]A/64/386 [5]A/65/405 [6]A/66/407

THE COMPOSITION OF **UN GGE**



NATIONAL REPLIES 1999-2011



[1]A/54/213 [2]A/55/140 and Add.1 [3]A/56/164 and Add.1 [4]A/57/166 and Add.1 [5]A/58/373 [6]A/59/116 and Add.1 [7]A/60/95 and Add.1 [8]A/61/161 and Add.1 [9]A/62/98 and Add.1
[10]A/63/139 [11]A/64/129 and Add.1 [12]A/65/154 [13]A/66/152 and Add.1

ICT4Peace
www.ict4peace.org

ICT4Peace was launched as a result of the World Summit on the Information Society in Geneva in 2003 and aims to facilitate improved, effective and sustained communication between peoples, communities and stakeholders involved in conflict prevention, mediation and peace building through better understanding of and enhanced application of Information Communications Technology (ICT). The ICT4Peace Cyber Security Program was started in 2011. We are interested in following, supporting and leading bilateral and multilateral diplomatic, legal and policy efforts to achieve a secure, prosperous and open cyberspace. The first phase of ICT4Peace activities in the field involves briefing of key processes shaping approaches to international cyber security.

Eneken Tikk-Ringas
enekentikk@ict4peace.org
+372 507 2270

Eneken Tikk-Ringas holds a PhD in law from Tartu University in Estonia since 2011. During her studies in Estonia, Sweden, Finland, Germany and the United States she has conducted extensive research in the field of IT and law, including data protection, electronic communications, cyber defense and cyber security.

Currently a post-doctoral fellow at the Citizen Lab, University of Toronto, Dr. Tikk-Ringas is advising the ICT4Peace Foundation on strategic legal and policy aspects of cyber security. Prior to her current assignments she served as legal adviser and acting head of the Legal and Policy Branch at NATO Cooperative Cyber Defence Centre of Excellence.

Her former professional tasks include heading the Estonian MOD's Cyber Defence Legal Expert Team tasked with the analysis of Estonian cyber security law in response to 2007 cyber attacks against Estonia, being part of the team drafting the Estonian cyber security strategy in 2008 and leading the development of the legislation for Estonian access to Schengen at the Estonian Ministry of Justice.

Dr. Tikk-Ringas has extensive teaching experience with Swedish National Defense College, Tallinn Technical University, Tartu University, Estonian Business School, Estonian Academy of State Defence and Estonian Military Academy. She has published numerous articles and books in her field of expertise.

ICT for peace
FOUNDATION